Hacking

This article is more than **1 year old**

Signal founder: I hacked police phone-cracking tool Cellebrite

Moxie Marlinspike accuses surveillance firm of being 'linked to persecution' around the world

Alex Hern *Technology editor*

@alexhern

Thu 22 Apr 2021 12.33 EDT

The CEO of the messaging app Signal claims to have hacked the phone-cracking tools used by police in Britain and around the world to extract information from seized devices.

In an online post, Moxie Marlinspike, the security researcher who founded Signal in 2013, detailed a series of vulnerabilities in the surveillance devices, made by the Israeli company Cellebrite.

Marlinspike says those weaknesses make it easy for anyone to plant code on a phone that would take over Cellebrite's hardware if it was used to scan the device. It would not only be able to silently affect all future investigations, but also to rewrite the data the tools had saved from previous analyses.

Marlinspike has been an outspoken critic of Cellebrite since the company claimed to be able to "break Signal encryption", a claim the hacker has dismissed. "Cellebrite makes software to automate physically extracting and indexing data from mobile devices," he says. "Their customer list has included authoritarian regimes in Belarus, Russia, Venezuela and China; death squads in Bangladesh; military juntas in Myanmar; and those seeking to abuse and oppress in Turkey, UAE and elsewhere.

"Their products have often been linked to the persecution of imprisoned journalists and activists around the world, but less has been written about what their software actually does or how it works."

Police forces around the world use Cellebrite's technology to help in digital investigations, particularly when they have managed to get hold of a physical device owned by a suspect or person of interest. While Cellebrite has been linked with attempts to bypass encrypted devices, the majority of its tools are built to allow digital forensics teams to extract information from unlocked, powered-on devices,

and automate the sort of searches they could theoretically do by hand on the phone itself.

But through reverse-engineering one Cellebrite device (Marlinspike claims he acquired the device "when I saw a small package fall off a truck ahead of me"), Signal's founder says he found more than 100 security vulnerabilities, just one of which could modify "not just the Cellebrite report being created in that scan, but also all previous and future generated Cellebrite reports from all previously scanned devices and all future scanned devices."

"Any app could contain such a file, and until Cellebrite is able to accurately repair all vulnerabilities in its software with extremely high confidence, the only remedy a Cellebrite user has is to not scan devices," Marlinspike says. In a winking suggestion that his company has placed such a booby-trap inside its own app, Marlinspike adds that "in completely unrelated news, upcoming versions of Signal will be periodically fetching files to place in app storage. These files are never used for anything inside Signal and never interact with Signal software or data, but they look nice, and aesthetics are important in software."

In a statement, Cellebrite said: "Cellebrite enables customers to protect and save lives, accelerate justice and preserve privacy in legally sanctioned investigations. We have strict licensing policies that govern how customers are permitted to use our technology and do not sell to countries under sanction by the US, Israel or the broader international community. Cellebrite is committed to protecting the integrity of our customers' data, and we continually

audit and update our software in order to equip our customers with the best digital intelligence solutions available."
